

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КІБЕРЗАХИСТУ

К.т.н., доц., Ю.П.Горелов Харківський національний університет внутрішніх справ, Харків

Відповідно до сучасних поглядів перспективна система кіберзахисту повинна бути взаємопов'язаною, багаторівневою та безупинно контролюваною системою, здатною оперативно реагувати на віддалені й локальні кібератаки та несанкціоновані дії, накопичувати знання про способи протидії, виявлення та реагування на атаки й несанкціоновані дії та використовувати їх для посилення захисту. Така система повинна надавати, принаймні, три рівні захисту. Перший рівень захисту становлять «традиційні» засоби захисту, що реалізують функції ідентифікації й аутентифікації, криптографічного захисту, розмежування доступу, контролю цілісності, реєстрації й обліку, міжмережевого екранування. Другий рівень включає засоби проактивного захисту, що забезпечують збір необхідної інформації, аналіз захищеності, моніторинг стану мережі, виявлення атак, протидію їхньої реалізації, введення зловмисника в оману й т.п. Третій рівень відповідає засобам керування захистом, які здійснюють інтегральну оцінку стану мережі, керування захистом й адаптацію політик безпеки й компонентів системи кіберзахисту. У доповіді розглядаються питання розробки сучасної системи кіберзахисту трирівневої архітектури з використанням методів та засобів штучного інтелекту.